Amendments to the Drawings:

The attached sheets of drawings include Replacement Sheets (formal drawings).

Attachment: Replacement Sheet

REMARKS

In response to the objection to the Abstract of the Disclosure, the Abstract has been amended to shorten it to less than 150 words. A copy of the amended Abstract is attached hereto on a separate sheet, as required.

The claims have been amended in order to place them in a format more consistent with U.S. practice, and to correct the spelling to conform with American English usage. In addition, Claim 1 has been amended at line 6 to provide an antecedent basis for the "user's mobile telephone" which is recited in lines 13 and 14. None of the amendments, however, alters the scope of the claims.

Formal drawings, labeled as "Replacement Sheets" are also submitted herewith.

Claims 1-9 have been rejected under 35 U.S.C. §103(a) as unpatentable over Turunen (European patent document EP 0 944 203 A2) in view of Salo et al (U.S. Patent No. 6,563,800) and Mouly et al, "*GSM System for Mobile Communications*". However, for the reasons set forth hereinafter, Applicants respectfully submit that all claims of record in this application distinguish over the cited references, whether considered separately or in combination.

The present invention is directed to a system for permitting a user, who is a subscriber with one network, to gain access as a "visitor" to one or more other W-LAN sites. The operator of the visited W-LAN site, however, must be assured of the bona fides and creditworthiness of the visitor before providing the visitor with services or information. Accordingly, one object of the invention is to achieve a subscription of a mobile user in a visiting wireless network, by which a billing of the exchange traffic is insured, and by which the subscription can be carried out in an "ad hoc manner" (meaning that the visiting mobile user is not necessarily required to become a registered user of the visited wireless network).

For the latter purpose, the present invention is based on the assumption that the visiting mobile user possesses a wireless computer terminal and has a valid subscription with a network, which is referred to as his "home network". In addition, it is also assumed that the visiting mobile user is a registered user of a cellular mobile phone account. The existence of the user's mobile cellular account is used by the system to provide the necessary verification of the user's identity, thereby encouraging a W-LAN operator to provide, for example, extra secure services to that user. Thus, the SIM (Subscriber Identity Module) card of the mobile user's cellular telephone acts effectively as a certificate of trust between the mobile user and the network operator. Successful receipt by the user of a short message via the GSM or other short message service (SMS) proves ownership of the SIM card and hence identify of the user, without requiring a third party or manual intervention by the W-LAN operator.

In summary, the system according to the invention achieves the object of access authentication by a method that conveys identity information to the home network server, which returns a personal identification number (PIN) to the mobile phone of the user. Provided with these two pieces of information (the identity information together with the PIN) by the visiting user, a server of the visiting network grants access for exchanging data traffic with a computer terminal of the mobile user. The prerequisite for such a grant (a valid billing account) is then met, because the cost of data traffic and the visited network can be charged to the visitor's cellular mobile telephone account.

In somewhat more detail, the PIN, which is generated by the home LAN, is transmitted to the mobile phone of the mobile visiting user, preferably using an SMS message in a supplementary mobile connection, in order to authenticate the visiting mobile user to the visited LAN, upon request of the visitor. Such authentication is used to confirm to the visited LAN that the visiting mobile user is entitled to exchange data in the visited LAN, and that the charges may be billed to the visitor's cellular mobile account. In other words, the information provided to the visited LAN is sufficient to establish the bona fides and creditworthiness of the visitor, based on the visitor's cellular mobile account, as noted previously.

The Turunen reference, on the other hand, discloses a method of enabling roaming of a mobile "host" from a local area network to a GSM network. As used

in Turunen, the term "host" refers to an interface to the Internet, which is typically a personal computer, as indicated, for example, at Column 1, lines 10-11. The term "roaming" denotes a seamless handover of a data communication system, when changing from a first network to a second network. For this purpose, a so-called "c/o address" (a temporary address for the mobile host that enables message delivery when it is connecting from somewhere other than its home network) is used. The c/o address identifies a mobile host's current point of attachment to a home agent, and makes it possible to connect from a different location, without changing the host's home address. This process is thus similar to the manner in which the postal system forwards letters through a "c/o address": Messages sent to the known permanent address are rerouted to the c/o address while the recipient can be reached there.

In order to achieve a higher security for transmitting the c/o address along with authentication data, Turunen proposes to send a security key from the home server (here, the remote station) over a cellular radio telephone network to the mobile host. Sending this key over the cellular radio telephone (GSM) network (for example, via a Short Message Service) instead of the Internet avoids an insecure Internet transmission which could be intercepted by a third party. In other words, the method according to Turunen treats a seamless linking of the mobile host with the remote station over the Internet, and a supplementary connection over the cellular mobile phone to transfer a security

key in order to secure the transmission of the c/o address and subsequent data transmissions between the mobile host and the remote station over the Internet.

The method according to Turunen thus provides for deregistering of the mobile terminal or host 9 from its home LAN 3 and registering it with the GSM network 6, where it receives a new Internet address, as indicated in the Abstract of the Disclosure.

For the purpose of the present discussion, the term "mobile host" of Turunen is assumed to be comparable to the "visitor" including the visitor's functional elements, according to the present invention as defined in Claim 1. In addition, the "remote station" (Claim 1 of Turunen) and the "home agent HA" in the corporate LAN 3 in Figure 3 of Turunen are assumed to be comparable to the "home server" in the specification of the present application. The "visitor server" according to the present invention is assumed to be comparable to the home agent (HA) of the "foreign" (GSM) network 6 in Figure 3 of Turunen.

The present invention as defined in Claim 1 distinguishes over Turunen in several respects. First, Turunen does not disclose a step of conveying an identity information by user intervention. Rather, because the object of a roaming procedure is a seamless handover, a user intervention would not be acceptable in the teaching of Turunen, in order to achieve this object. Accordingly, it is not the user which registers with the foreign agent (FA) of Turunen, line 10, but rather the mobile host. (See Turunen, Column 2, lines 35 *et seq.*) In this regard,

Applicants note that it is clear from the specification of the present application that the term "user" refers to an individual who is the owner of a mobile telephone and has a mobile telephone account. (See, for example, page 3, lines 1-16; page 4, line 15 - page 5, line 2; page 6, lines 3-9; and page 9, lines 15-18.)

Furthermore, Turunen also fails to teach or suggest conveying identity information in order to enable the visitor server to communicate with the home server. Rather, according to paragraph [0008] of Turunen, the mobile host, on entering the foreign networks, sends its new Internet address (if the latter is considered to constitute identity information), assigned by the foreign agent, to its home agent. During the roaming, the mobile host retains permanent knowledge of the identity information, *i.e.*, address, of its home agent. Thus, there is no need, and therefore no motivation, for the foreign agent of Turunen to communicate with the home agent for the purpose of conveying an identity information. A GSM data exchange between the home agent as shown in Figure 3 (reference numeral 11) of Turunen does also not disclose conveying an identity information for the purpose of enabling the visitor server to communicate with the home server, because it is a prerequisite of the used point-to-point network GSM that the communications partners (mobile host and home agent) know the identity (in the present case, in terms of the telephone number for transmitting and SMS) of each other. (See paragraphs [0017] and [0030].)

Turunen discloses an authentication key/personal identification number (referred to as a PIN in the following), which is sent to the mobile host. In Turunen, however, the PIN is used to secure the transmission of the c/o address and subsequent data transmission between the mobile host and the remote station over the Internet. Turunen does not disclose that this PIN is used for authenticating access to the foreign network as provided in the present invention.

The Salo et al reference, on the other hand, discloses the use of a PIN to gain network access. However, Applicants respectfully submit that there is no motivation to use a PIN (or in particular, the PIN of Turunen) in order to gain access to the foreign network of Turunen, as assumed in the Office Action. Rather, the foreign networks (Figure 3, numerals 6, 7, 8) outside the corporate LAN (Figure 3, numeral 3) are either "hot spots" which are open for public use, or are operated by cellular network operators (paragraph [0006], lines 16-17), where the access of a mobile host in the form of a cellular telephone is handled by lower GSM protocol layers using the SIM card information of that cellular telephone. Hence, there is no motivation to gain access to the foreign network via a PIN in Turunen, because it is presumed that those networks are inherently accessible in order to allow a seamless handover.

As indicated in the Office Action, the Mouly reference discloses that access to a GSM network may be billed to the account of the GSM network. That is, the

access and the billing are effected in the same network. However, it is an essential feature of the present invention according to Claim 1 that the access to the visited W-LAN is billed to the user's cellular mobile account. That is, the access to a first network (visited W-LAN) is billed to an account of a second network (GSM network) which is different from the first network. The invention thus provides a method of gaining access to a foreign network by entering validated information about an alternative account. The alternative account in this case is the user's cellular mobile account. More importantly, it is neither his account with the home network nor an account with a foreign W-LAN. Accordingly, this feature of the invention, which is neither taught nor suggested by any of the references, enables the system according to the invention to permit a visiting user to gain access on an ad hoc basis (that is, without being required to become a registered user of the visited wireless network).

Turunen does not disclose a billing of access costs to an account which is different from the "home" account. Rather, it uses the "classical" GSM technique when roaming a cellular mobile device between different networks: for billing purposes, the home network account is always charged. Moreover, Mouly does not teach or suggest billing to an alternative account as described above, since the disclose of Mouly deals with the well known GSM techniques for roaming a mobile telephone connection while billing the charges to the user's account of that network that is accessed.

For the reasons set forth above, Applicants respectfully submit that independent Claim 1, the only independent claim of record, distinguishes over the cited combination of Turunen, Salo et al and Mouly.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket #3036/50289).

Respectfully submitted,

Gary R. Edwards
Registration No. 31,824

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:kms
Attachments – Replacement Sheets (Formal Drawings)
391468v1